

REMARKS

Claims 1, 3-8, 10-16, and 18 are currently pending in this application. By this amendment, claims 1, 7, 10, and 12 are amended, and claim 9 is canceled without prejudice. Support for the amendments is found in the specification, including the claims, as originally filed. No new matter has been introduced. Favorable reconsideration of the application in light of the foregoing amendments and following comments is respectfully solicited.

Rejection Under 35 U.S.C. § 112, First Paragraph

In section 7 of the Office Action, claims 1 and 3-9 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Applicants respectfully traverse.

Page 3 of the Office Action indicates “the examiner is unable to find any support that data is transmitted in a time division manner.” Independent claims 1 and 7 are each amended to remove the phrase “and in a time-division manner.” Applicants respectfully submit the claims comply with Section 112, and request withdrawal of the rejection.

Rejections Under 35 U.S.C. § 103(a)

In section 9 of the Office Action, claims 1, 3-5, 7, 8, 10-16, and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,158,637 (Ohta) in view of U.S. Patent No. 6,275,909 (Arimilli) and U.S. Patent No. 4,238,854 (Ehram). In section 28 of the Office Action, claims 6 and 9 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohta in view of Arimilli, Ehram, and U.S. Patent App. Pub. No. 2003/0226029 (Porter). Applicants respectfully traverse.

Amended independent claim 1 recites, *inter alia*,

- an ordinary data storage unit which stores encrypted contents data;
- a secret data storage unit which stores license data containing a contents key for decrypting the encrypted contents data;
- a cryptographic processing unit which receives, from a host device, and executes a command corresponding to each of a plurality of sequenced subprocesses produced by dividing each of a series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data between the storage device and the host device;
- a controller which inputs and outputs the license data via the cryptographic processing unit and inputs and outputs the encrypted contents data bypassing the cryptographic processing unit;

...

wherein the cryptographic processing unit receives commands corresponding to a plurality of subprocesses respectively belonging to two or more different cryptographic input and output processes via the bus, refers to identifying information attached to the command, identifies to which cryptographic input and output process the command belongs, manages the sequence of commands executed in each cryptographic input and output process, and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command.

Ohta, Arimilli, Ehrsam, and Porter, individually or in combination, do not render obvious the recited limitations.

Amended independent claim 7 recites, *inter alia*,

- an ordinary data storage unit which stores encrypted contents data;
- a secret data storage unit which stores license data containing a contents key for decrypting the encrypted contents data;
- a cryptographic processing unit for receiving, from a host device, and executing a command corresponding to each of the plurality of sequenced subprocesses produced by dividing each of a series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data between the storage device and the host device;
- a controller which inputs and outputs the license data via the cryptographic processing unit and inputs and outputs the encrypted contents data bypassing the cryptographic processing unit;

...

wherein the cryptographic processing unit receives commands corresponding to a plurality of subprocesses respectively belonging to two or more different cryptographic input and output processes via the bus, refers to identifying information attached to the command, identifies to which cryptographic input and output process the received command belongs to, and

rejects the execution of the command when having detected that the command is an incorrectly sequenced command in the cryptographic input and output process to which the command belongs.

Ohta, Arimilli, Ehram, and Porter, individually or in combination, do not render obvious the recited limitations.

Amended independent claim 10 recites, *inter alia*,

[a] host device which exchanges encrypted contents data and license data containing a contents key for decrypting the encrypted contents data, with a storage device that is capable of simultaneously performing a plurality of series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data, the host device comprising:

a controller which divides the cryptographic input and output process into a plurality of sequenced subprocesses and issues commands sequentially to the storage device thereby allowing the storage device to execute a subprocess to be executed on the storage-device side; and

a cryptographic processing unit which carries out encryption or decryption that is required of the cryptographic input and output process, wherein

the controller inputs and outputs the license data via the cryptographic processing unit and inputs and outputs the encrypted contents data bypassing the cryptographic processing unit, and

when the controller issues a command, the controller attaches identifying information to the command to identify to which one of the plurality of cryptographic input and output processes the command belongs and to manage the sequence of commands executed in each cryptographic input and output process.

Ohta, Arimilli, Ehram, and Porter, individually or in combination, do not render obvious the recited limitations.

Amended independent claim 12 recites, *inter alia*,

exchanging encrypted contents data and license data containing a contents key for decrypting the encrypted contents data between a storage device and a host device, wherein, when performing a cryptographic input and output process between the host device and the storage device, which is capable of simultaneously performing a plurality of series of cryptographic input and output processes for encrypting data to be secured and inputting and outputting the data, the license data is input and output through the cryptographic input and output process, and the encrypted data is input and output bypassing the cryptographic input and output process

...

identifying information is attached to the command to identify to which one of the plurality of cryptographic input and output processes, being performed simultaneously by the storage device, the command belongs;

...

determining whether the received command is a correctly sequenced command in the cryptographic input and output process;

accepting the command successfully when the received command has been determined to be a correctly sequenced command; and

rejecting the execution of the received command when the received command has been determined to be an incorrectly sequenced command.

Ohta, Arimilli, Ehram, and Porter, individually or in combination, do not render obvious the recited limitations.

As none of the independent claims are rendered obvious by the cited art, Applicants respectfully request withdrawal of the rejections of the claims under Section 103.

Conclusion

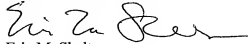
In view of the above amendments and remarks, Applicants submit that this application should be allowed and the case passed to issue. If there are any questions regarding this Amendment or the application in general, a telephone call to the undersigned would be appreciated to expedite the prosecution of the application.

Application No.: 10/889,815

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Eric M. Shelton

Registration No. 57,630

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 BPC/EMS:amz
Facsimile: 202.756.8087
Date: November 13, 2009

**Please recognize our Customer No. 20277
as our correspondence address.**